Fake news: a technological approach to proving the origins of content, using blockchains

Article (Published Version)

BIG DATA

Big Data

Fake News - a Technological Approach to Proving the Origins of Content, Using Blockchains

Journal:	*Big Data*
Manuscript ID	BIG-2017-0071.R2
Manuscript Type:	Original Article
Date Submitted by the Author:	31-Oct-2017
Complete List of Authors:	Huckle, Steve; University of Sussex, School of Engineering and Informatics White, Martin; University of Sussex, School of Engineering and Informatics
Keywords:	Big data analytics, Big data infrastructure design, Data mining, data protection, privacy, and policy, Semi-structured data
Manuscript Keywords (Search Terms):	Fake News, Ethereum, Blockchain, Cryptography, PREMIS, Hash functions

Fake News - a Technological Approach to Proving the Origins of Content, Using Blockchains

Steve Huckle [1]*, Martin White [1]

1 University of Sussex, Sussex House, Falmer, Brighton, BN1 9RH, United Kingdom

* Direct comments to: s.huckle@sussex.ac.uk; Tel.: +44 (0)1273 606755

Abstract

In this paper, we introduce a prototype of an innovative technology for proving the origins of captured digital media. In an era of fake news, when someone shows us a video or picture of some event, how can we trust its authenticity? It seems the public no longer believe that traditional media is a reliable reference of fact, perhaps due, in part, to the onset of many diverse sources of conflicting information, via social media. Indeed, the issue of 'fake' reached a crescendo during the 2016 US Presidential Election, when the winner, Donald Trump, claimed that the New York Times was trying to discredit him by pushing disinformation. Current research into overcoming the problem of fake news does not focus on establishing the ownership of media resources used in such stories - the blockchain-based application introduced in this article is technology that is capable of indicating the authenticity of digital media. Put simply; by using the trust mechanisms of blockchain technology, the tool can show, beyond doubt, the provenance of any source of digital media, including images used out of context in attempts to mislead. Although the application is an early prototype and its capability to find fake resources is

somewhat limited, we outline future improvements that would overcome such limitations. Furthermore, we believe our application (and its use of blockchain technology and standardised metadata), introduces a novel approach to overcoming falsities in news reporting and the provenance of media resources used therein. However, while our application has the potential to be able to verify the originality of media resources, we believe technology is only capable of providing a partial solution to fake news. That is because it is incapable of proving the authenticity of a news story as a whole. We believe that takes human skills.

Keywords: Fake News, blockchain, big data, Ethereum, hash functions, cryptography, public-key cryptography, digital signatures, Preservation Metadata

Introduction

The issue of fake news hit the headlines when Donald Trump, the winner of the 2016 U.S. Presidential Election, accused various media outlets of mounting a concerted effort to discredit him[1] by publishing hoaxes and propaganda[2]. Even before the President's accusations, one of the implicated newspapers, The New York Times, printed a story asserting that one of Trump's prominent supporters was spreading disinformation[3]. After, presumably, much journalistic investigation, the newspaper claimed falsehood by showing that a photograph (illustrated in Figure 1), which was used on the Christian Times website to suggest that the US President's opponents were rigging votes, was, in fact, a picture from the UK's Birmingham Mail. The picture showed ballot boxes used in a UK election, not fraudulent Clinton votes found in an Ohio Warehouse, as the website claimed. However, what if such

detective work was unnecessary? What if it were trivial to ascertain the provenance of a picture or video? Not only could we trust that material, but we could distrust any material that was not validated that way.

Figure 1. Birmingham Mail picture of the delivery of ballot boxes used in a UK election. The picture was misappropriated by a Trump supporter, who (falsely) claimed that the image showed that the Clinton campaign team were rigging votes[4]

The primary aim of this article is to introduce a blockchain-based distributed application that we are calling Provenator (intended as the agent noun of the verb form of provenance, which means establishing the origin of something), a tool that helps prove the originator of media sources. Before describing Provenator, we provide some background by introducing the motivation for this work - fake news. Then we present big data's role in technological attempts to counter false reporting. Next, we describe the technologies underlying Provenator - blockchains and a data schema for recording metadata about media resources. Then we discuss Provenator

in detail, including its use, current limitations and future improvements that might address those limitations, before concluding.

Fake News

Fake News is, quite simply, invented information[5]. Unfortunately, it is often difficult to spot invented from real. For instance, in a recent survey, when the UK's Channel 4 News showed three real and three fake stories to 1,684 adults, only 4% of the respondents were able to identify all the stories correctly, and nearly half thought that at least one of the fakes was real[6].

While the Channel 4 survey may not appear, at first glance, to raise a major issue, a somewhat more nuanced interpretation of fake news is that they are stories that are distorted or decontextualised and deliberately designed to deceive. Often, such stories have an undeclared political bias[5]. Thus, fake news is a synonym for propaganda, a term which has sinister connotations. As an example, during the recent annexation of the Crimea, NATO accused Russia of using fake news to spread disinformation about their actions there[7]. Moreover, in a follow-up to their survey, Channel 4 ran a news series on fake news, in which they interviewed Janis Sartis, the Director of the NATO Strategic Communications Centre. During the interview, Sartis said: "You don't need tanks. You might actually achieve your goals if you change the perception of a given society in a way that corresponds to your interests and the society starts to act how you want them to act"[8].

Social media companies have come under political pressure for not providing tools to counter the problem of fake news. Consequently, politicians have accused those

companies of having an undue influence on elections both in the UK and U.S.[9]. Indeed, analysis has shown that, during the final three months of the U.S. presidential campaign, Facebook's fake news stories about the U.S. presidential election generated much more interest than stories from traditional news outlets[10]. Indeed, Facebook admitted that: "more and more…debate is mirrored online on platforms like Facebook, leading to an increase in individual access and agency in political dialogue…as well as the diversity of influences on any given conversation"[11]. To counter this issue, Facebook placed advertisements in UK newspapers, giving tips to its users on how to spot fake news items[12]. The company also implemented several design features on its platform's user interface; measures included stronger automated detection of fakes, convenient user reporting of suspicious content and third-party verification of news items[13]. The founder of Wikipedia, James Wales, also announced a new initiative for countering fake news[14].

The criticisms of social media platforms and fake news suggest that the issue is a new phenomenon. However, propaganda has a long history.

A Brief History of Fake News

During a recent TED talk, Yuval Noah Harari said: "I think fake news has been with us a long time; just think of the Bible!"[15]. Indeed, the earliest example of propaganda is considered to be the Behistun Inscription, authored around 515 BC, which is an inscription in three different cuniform dialects on a cliff at Mount Behistun in Kermanshah Province, Western Iran. It details the rise to the throne of the Persian Empire of Darius I and his success in quelling multiple rebellions[16]. However, Pope

Gregory XV was the first to use the term 'propaganda', when in 1622, he formed the 'Congregatio de Propaganda Fide', or "congregation for propagating the faith." The word itself comes from the Latin word 'propagare', meaning propagation. Hence, propaganda is understood to mean the propagation of an ideology[17].

A more modern example of propaganda, yet still one-hundred years old, was described by Dr David Clarke in a recent piece for the BBC[18]. Dr Clarke tells how, in 1917, the British Government, in an ultimately successful attempt to bring China onto the Allied side in The Great War, fabricated a gruesome story about the German military, whom they (falsely) accused of extracting glycerine from human corpses. Apparently, Conservative MP John Charteris, Head of Intelligence at the time of the story's fabrication, transposed captions from a photograph that showed a train of dead horses that were to be rendered onto another showing a train taking dead soldiers for burial. Unfortunately, the story was later used by the Nazi Party as proof of British lies during the Great War, and it may have led to doubts about news of Nazi atrocities during the Second World War; as Dr Clarke comments: "lies have consequences"[18]. The Nazi Party, realising the importance of war propaganda, formed the Reich Ministry of Public Enlightenment and Propaganda. The Ministry's head, Joseph Goebbels, used his control of the press to help reinforce Nazi ideology through fake news: "If you tell the same lie enough times, people will believe it; and the bigger the lie, the better"[19].

Much like Nazi Germany, Stalinist Russia, in an attempt to convince its people that the Soviet Union enjoyed much higher living standards than those in the Capitalist West, used propaganda extensively[20]. During the lead-up to the Second World War,

the Soviet media suppressed heretical opinion through the censorship of dissonant voices. Newspaper headlines took a standard form: “all workers greeted the policy (of the Russian Government) with satisfaction.” They repeated the message often, giving credence to Goebbels’ mantra that if you tell a lie often enough, people will believe it. Soviet propaganda continued after the war too, with books heavily censored and newspapers propagating ideolised reality[21]. Television and radio gave that reality a degree of formality. Meanwhile, cinematography took a triumphalist tone, depicting happy lives and the fulfilment of the ‘Soviet dream’[21].

Despite increasing press freedom in the 1990s, following Glasnost (a Soviet policy of open discussion of political and social issues), Russian authorities appear to continue propagating fake news stories. Indeed, on February 22nd, 2017, the Russian Minister of Defence, Sergei Shoigu, admitted that four years prior, the Russian Government had established ‘Voyska Informatsionnykh Operatsiy,’ a dedicated information warfare force, because: “Our propaganda needs to be clever, smart and efficient”[22]. For instance, they may deliberately take images out of context so that they support the state narrative[23]. For example, to refute the Western narrative that the passenger aircraft MH17 was shot down by Russian-backed Ukrainian Separatists, Russian state television has reported on an ariel photograph of a jet fighter firing a missile at the downed plane. However, an organisation called StopFake has gone to great lengths to debunk the picture, citing evidence such as the incorrect placement of the Malaysian Airlines logo and the lack of aircraft vapour trails[23].

The Russian State has not been the sole purveyors of fake news in the modern world. In 1928, Cornell Graduate Edward Bernays published a book called *Propaganda*, which has become, essentially, a manual of mass manipulation[24]. The book opens with the following paragraph: "The conscious and intelligent manipulation of the organized habits and opinions of the masses is an important element in a democratic society. Those who manipulate this unseen mechanism of society constitute an invisible government which is the true ruling power of our country." In fact, before the First World War, the term propaganda was not used negatively, but the public began to mistrust the term once they realised the extent to which the Anglo-American political machinery had deployed propaganda in an attempt to demonise "The Hun"[24]. Its use by the Nazi Party in the Second World War[25], and later by Communist Russia, appears to have sealed the term's fate; now propaganda has extremely negative connotations. However, that does not mean that its use in the West has diminished. Immediately after the war, U.S. President Truman instigated NSC/10, a policy to contain the Soviet state using wide-ranging covert operations, including propaganda[26]. During the 1960s and 1970s, the media corporations of Western nations were instrumental in promoting neo-colonialism (the practice of exerting influence or control over less developed countries by using trade policies, economic or financial means) and incapacitating attempts at self-determination by third world countries[25]. There are recent examples of Western propaganda too; in 2005, the U.S. Government tried to sway public opinion as to the benefits of the Iraq War by spending US$300 million on an initiative to propagate 'positive news'[27].

Democracy and the Free Press

Perhaps the most famous example of fake news from the literary fiction is George Orwell's Nineteen Eighty-Four[28]. The book depicts the Inner Party, a tyrannical organisation who govern a Super State. One of the novel's main themes is censorship through the Inner Party's modification of records, such as photographs. The protagonist is Winston Smith, who works for the Ministry of Truth; it is his job to re-write past newspaper articles and thereby distort records so that they correspond to the party's propaganda. By depicting a state that enforces suppression through historical revisionism, Orwell demonstrates that press freedom is core to the healthy functioning of a democratic nation. Undoubtedly, a free press plays a pivotal role in a democracy's political culture because it relies upon a "healthy and vibrant" media system, who keep its citizens adequately informed[25]. Indeed, the media's ownership, management and funding directly affect its capacity to serve the democratic process[25].

The President of the United States is the 'Leader of the Free World'. The 'Free World' includes nations who espouse certain freedoms, such as those based on a free press, and it is formed primarily by the countries who opposed both Fascism in the Second World War and Soviet Communism during the Cold War. Hence, the U.S. is at the zenith of all the supposed free, democratic nations. The First Amendment to the U.S. Constitution guarantees individual and press freedom by prohibiting government from impinging on those freedoms: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble,

and to petition the government for a redress of grievances"[29]. It is, then, somewhat disconcerting when the US President starts to undermine the free press by accusing them of spreading fake news. Coleen Christie, the host of Canada's CTV News, believes that the President's fake news accusation is merely a symptom of the explosion of digital media, which has changed our legacy news platforms and undermined our trust in such platforms[30]. Indeed, she warns that: "in this modern news age, information is power, yet never has our ability to leverage that power been more at risk." As we have already seen, social media outlets are coming under increasing political pressure to ensure the integrity of the items published on their platforms, so they have started to implement measures to help counter the phenomenon. Could new digital technologies help rather than hinder? Might blockchains provide methods for circumventing the issue of fake news by establishing the credentials (or not) of media resources used in such stories? Much of the rest of this paper discusses such a possibility. However, first, we describe some ongoing research into big data and fake news.

Big Data and Fake News

Big data refers not just to the large quantities of digital data, but also to the quality of the data and the relationships formed[31]. In other words, big data is networked, and recognising patterns therein creates value. Unfortunately, as we have shown above, the data may not always reflect the truth[32]. Hence, even if big data has the potential to transform our understanding of world events[31], there are dangers presented by inaccuracies and/or (deliberate) falsities[33]. Indeed, news, in its purest sense, is meant to convey truthful, unbiased and informative facts about issues

affecting the world. Hence, gathering reliable information is an important part of a journalist's skills[34]; they must take a critical perspective on all information collected because their stories must stand up to later scrutiny.

Library and information science is adapting to the challenges of big data news streams, by attempting to use automated methods for analysing text and verifying online information[33]: "separating the news from the noise is key to the verification of digital information"[35]. We take a look at some such initiatives next.

Fake News Detection Technologies

City University has instigated a project, sponsored by Google, with the goal of helping journalists identify fake news by analysing relationships in large, complex news-based datasets[35]. City is developing a web-based tool that combines machine learning and artificial intelligence technologies to visualise those relationships[35]. They are aiming to test their product with European-based news organisations, such as the UK's Telegraph media group and the Guardian, as well as Ireland's national broadcaster, RTE.

As we have already shown, nowadays, users don't get their news solely from traditional print and broadcast media; they also get it from social media sources. Hence, both Narwal et al.[36] and Jin et al.[37] focus their attention on overcoming fake news on platforms such as Twitter. Jin et al. describe a tool that analyses messages and creates a hierarchical graph optimisation of the relationship between news events. By so doing, their application propagates the credibility of those events[37]. Narwat et al. have developed a tool called UnbiasedCrowd, whose purpose is to,

first, identify bias, second, identify images that are used out of context to support a particular opinion, and third, create a call to action, whereby activists are urged to expose the inherent bias[36].

The application developed in this article, Provenator, stores provenance metadata on a blockchain, thus enabling content creators to prove, unequivocally, the origins of their media resources. Because of the properties of blockchains (which we will describe later), that also means users can trust the authenticity of the metadata about those resources. Additionally, Provenator provides an interface whereby users can check the provenance of media resources used in news stories. However, that supposes that Provenator was used to document the resource in the first place; in reality, that functionality is only useful given wide-scale deployment of our application. Of course, since we are at the prototype stage, that has yet to happen. However, such wide-scale use is possible, so later in the article, when we describe such a scenario, we feel justified in doing so.

Before we detail Provenator itself, we first describe the technologies it uses to help facilitate data integrity and authenticity.

Methods for Trust and Authenticity

As we have already discussed, it is crucial that reporters trust the integrity and authenticity of the media resources contained within their news stories. For example, suppose Alice is the Birmingham Mail Photographer who was responsible for the picture of the UK ballot boxes, which we discussed in the introduction. Imagine that Bob is her Picture Editor, who must be satisfied with the image's

integrity and authenticity. For instance, he has to be sure that, without Alice's knowledge, someone has not swapped the picture for another (or that any modifications have a verifiable provenance trail). We will show, to achieve such confidence, Bob requires methods from the field of cryptography.

Cryptography

Cryptography is the mathematics of information security[38], a field of study that investigates the confidentiality, integrity, authenticity and non-repudiation of data[39]. Next, we describe some tools that apply techniques from cryptography; namely, public-key cryptography, cryptographic hash functions and digital signatures.

Public-key Cryptography

Data encryption is a process that produces ciphertext by combining some original text (to be kept secret, for whatever reason), with a much shorter key. Later, it is possible to use the key to transform the ciphertext back into the original text, a process known as decryption[40].

Public-key cryptography (PKC) is a particular form of encryption that uses a pair of asymmetric keys; a private key that is known only to the owner and a public key that is widely shared[38]. The basic idea is that encryption is achieved using the public key and decryption using the private key[39]. Figure 2 shows how Alice could use public-key cryptography to send a secure message to Bob about her picture; she uses Bob's public key to encrypt the message, and subsequently, only Bob can decrypt Alice's message since he is the only person who has the paired private key.

Thus, the security of public-key cryptography systems relies upon the secrecy of the private key.

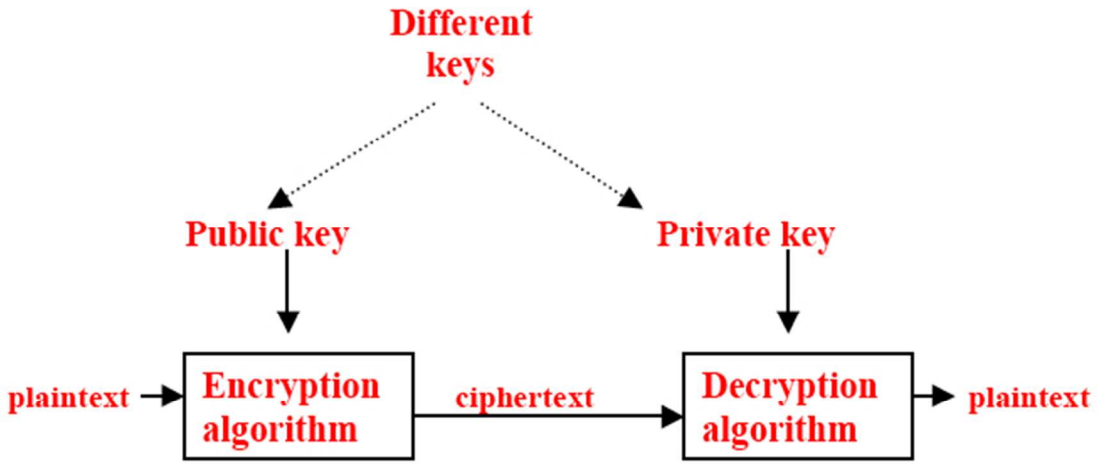


Figure 2. Public Key Cryptography[39]

Figure 3 shows the process Bob uses to generate his private and public keys; he feeds a random number into a key generation program, from which it produces the required keys.

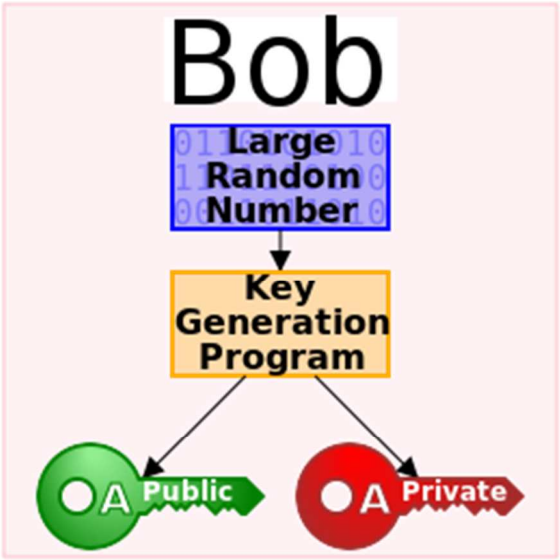


Figure 3. Key Generation[41]

In PKC systems, it is trivial (computationally) to generate public and private keys, but once the public key is known, it is infeasible to find the private key. That is a result of a class of mathematical problems that have no efficient solution. One such problem is the discrete logarithm, which uses the modular exponentiation of large prime numbers that are easy to compute, but practically impossible to invert[39].

Cryptographic Hash Functions

When Alice sends her photograph, Bob must be satisfied that, while in transit, it has remained unaltered. Cryptographic hash functions can help there. The basic idea is that Alice computes a cryptographic hash of the picture, which she then sends to Bob alongside the image itself. Bob then calculates the cryptographic hash value of the received photo and checks that the hash matches the value Alice sent.

A cryptographic hash is a one-way function that maps arbitrary data to a fixed-size string. They are mathematical algorithms that are infeasible to invert (much like their public-key cryptography counterparts). The ideal cryptographic hash function has five main properties:

1 Deterministic - the same message results in the same hash.

2 Fast - for any message, it is quick to calculate the hash.

3 One-way - it is practically impossible to generate the message from its hash.

4 No correlation - a small change to a message will drastically modify the hash.

5 Collision resistance - it is computationally infeasible to find any two distinct inputs, M and M *, which hash to the same value[39].

Figure 4 shows a hash function that converts an arbitrary length block of data into a unique, fixed-length, 'hash-value' that serves as a compact representation of the original data[39].

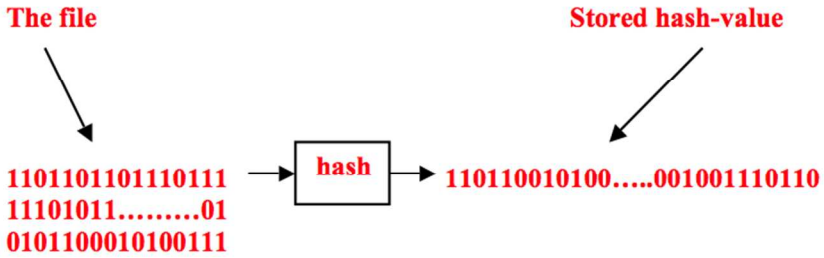


Figure 4. A Hash Function[39]

Figure 5 shows that, after receiving Alice's photograph, the hash Bob computes must be unique to a given input[42]. In other words, if the hash is the same as the original, then Alice's image must have remained unaltered.

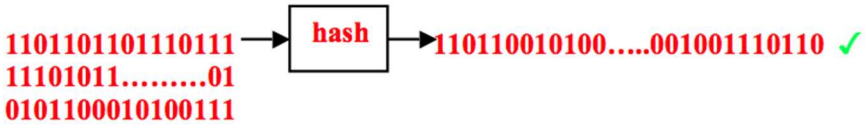


Figure 5. The Validated Hash[39]

Similarly, Figure 6 shows that if the hash generated by Bob does not match that sent by Alice, then the picture must have been modified.

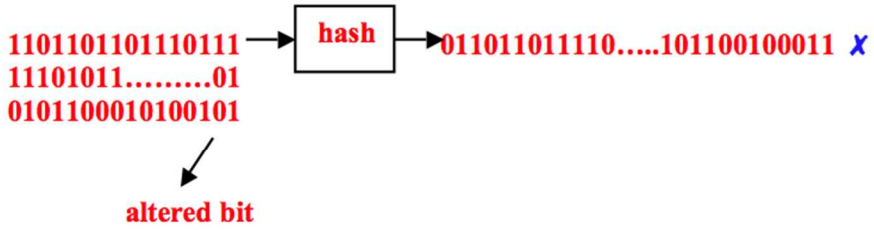


Figure 6. An Altered File[39]

An example hash function is SHA-256, which produces many fixed-size 256-bit (32-byte) hashes. For all practical purposes, finding collisions is beyond the capabilities

of present-day computing. It is an iterated hash function, a process shown in Figure 7; its design ensures the use of all message bits in the final hash value Hk. It works by splitting the input into a sequence of fixed-size blocks M1, M2, M3,..., Mk, with some padding rule for the last block Mk. Input blocks are processed in order, using a one-way compression function that gives a set of intermediate hash values H0, H1, H2,..., Hk. H0 is a predefined initialising value, and Hk is the hash value output of the SHA-256 function.

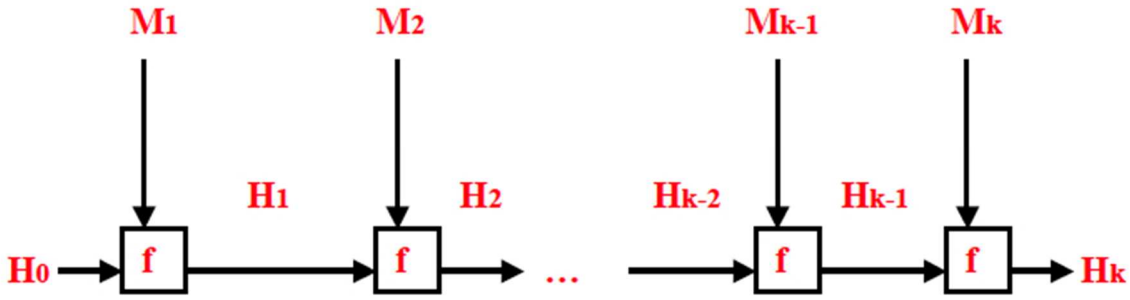


Figure 7. An Iterated Hash Function[39]

Earlier, while giving an overview of hashing functions, we showed that a computed hash must match that of the origin. However, that raises the problem of ensuring the validity of the original hash. In other words, Bob may question whether it was Alice who sent the hash of the picture in the first place. Digital signatures can help there. We discuss those next.

Digital Signatures

From an early age, we learn the importance of a written signature as it serves to identify, authorise and validate[38]. In the electronic world, it is trivial to append to a document a signature that does not belong to the originator, so cryptography has developed advanced digital signature techniques that would allow Alice to bind her

identity to her photograph. The process would involve Alice executing a transform so that the final message she sends to Bob combines the original image together with some secret information held only by Alice[38].

An overview of the digital signature process is shown in Figure 8. To allow Alice to share information with Bob (in a manner that guarantees the data's authenticity), she creates a signature that Bob can use to validate her message. Moreover, Alice would be unable to deny that it was she who shared the information, due to the non-repudiation properties of digital signatures.

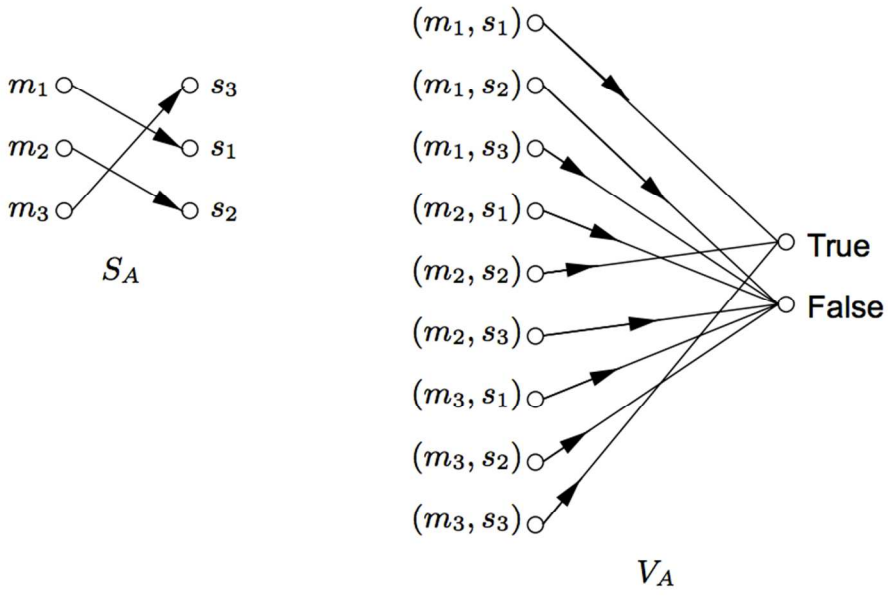


Figure 8. The Digital Signature Process.

- *M - the set of messages to be signed by Alice.*
- *S - a collection of Alice's signatures.*
- *SA - a secret signing transformation that will be used by Alice to create signatures from messages M.*
- *VA - a verification transformation, from the set M×S to the set {true, false}, for Alice's signatures. VA is publicly known, so Bob can use it to verify signatures created by Alice, thereby authenticating the messages they share[38].*

A typical usage of a digital signature is to sign a cryptographic hash of a message (the information that must be signed)[38], using the signees private key[43]. The signature then takes the form of a number that proves the signing operation took place.

Technologies Used by Provenator to Prove Authenticity

The application we are about to describe, Provenator, uses technologies that employ methods from cryptography to help determine the authenticity of media resources. Additionally, it uses a schema to record and retrieve metadata describing those media resources. We describe those technologies next.

Blockchains

Blockchains have capabilities resulting in their suitability for determining integrity and authenticity because they are, essentially, an immutable database technology[44] with inbuilt trust mechanisms[45]. They include cryptographic algorithms and digital signatures that allow secure electronic collaboration, without requiring any centralised authority[46]. Blockchains also have the ability to execute smart contracts, which are verifiable scripts that automate a system's rule set[47]. In essence, then, blockchains are a trusted ledger capable of running application logic[47]. Furthermore, they cannot be controlled by any single entity[48]. Those mechanisms mean we can use a blockchain to record data about our media resources and any entity that views those records will be satisfied that the information conveyed is authentic. However, we still require an appropriate schema for recording data on the blockchain. We discuss that next.

Provenance Metadata

PREMIS stands for "Preservation Metadata: Implementation Strategies"; it outlines a provenance schema which helps identify a resource[49]. The PREMIS data model[50], shown in Figure 9, describes four separate preservation entities: 1) Objects, 2) Events, 3) Agents and 4) Rights.

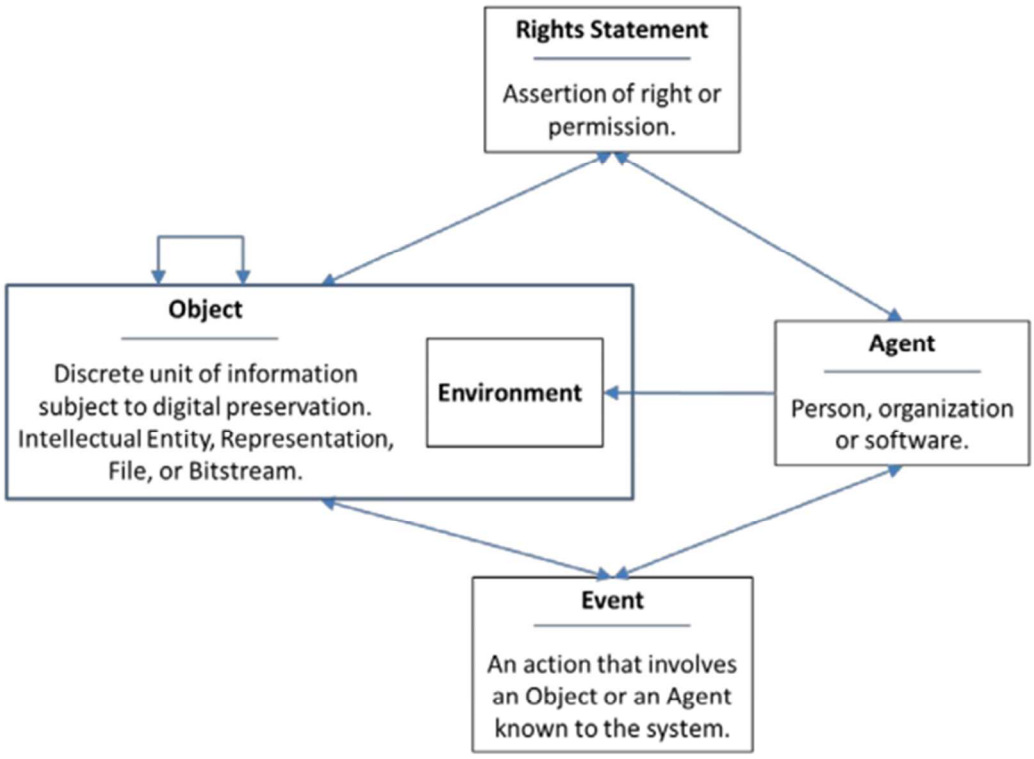


Figure 9. The PREMIS 3.0 data model[50]

Provenator uses PREMIS metadata definitions to record the provenance of digital media items on the blockchain, using smart contracts. That ensures the data conforms to an open standard, which should 'future-proof' the information held and help facilitate further interactions with different users[51]. It also develops some of the ideas of Mannens et al.[52], who propose using metadata, alongside descriptions,

to accompany news items because that would facilitate transparency and trust estimation.

The Provenator Application

The general principle of Provenator is that a content creator should be able to prove the provenance of the resources they create. To do so, Provenator gives creators the ability to store relevant authentication information about their creations on the blockchain so that it can be retrieved easily later and used to verify those same resources.

Requirements of the Provenator Application

We are almost in a position to discuss Provenator in detail. However, we still need to consider the steps required to prove the provenance metadata of media resources. Thankfully, we need not think of those steps ourselves, because a similar 'trust' process is employed when distributing new releases of the Ubuntu operating system software, which we describe next.

Distributing the Ubuntu Operating System Software

The steps for distributing Ubuntu, shown below, involve combining digital signatures with PKC to help ensure that the software downloaded and installed can be trusted. The process is as follows:

1 Download the operating system's disk image, together with a file of checksums and the signature used to sign the checksums file.

2 Fetch the public key used for the signature.

3 Use the key to verify the checksums file's signature.

4 Run a command that generates a SHA-256 cryptographic hash on the operating system disk image.

5 Check that the generated hash matches the hash from the downloaded checksums file[53].

Hence, by following the process above, if the hashes match, a user can install the operating system and trust that they have an official Ubuntu release. Indeed, Alice could use a similar process to share her image with Bob.

Operations of the Provenator Application

Borrowing from the Ubuntu process for verifying the Ubuntu software, Provenator should do the following:

1 Get a cryptographic hash of the digital media resource.

2 Create the PREMIS metadata of the digital resource.

3 Sign the transaction that stores the cryptographic hash of the digital resource, and its associated metadata, on the blockchain.

By following that process, subsequent users of the data will be able to trust the integrity and authenticity of the digital media metadata because of the immutability of blockchain records. Below shows how Provenator will allow such users to check a digital resource's provenance data on the blockchain:

1 Get a cryptographic hash of the digital resource.

2 Check whether that hash exists on the blockchain.

3 If the hash exists, retrieve the associated metadata.

Next, we will look in more detail at Provenator's architecture.

Provenator's Architecture

Provenator consists of the following architecture:

- An Ethereum blockchain[54], that stores the provenance metadata about media resources.
- Ethereum smart contracts, written in the language Solidity[55], which reads and writes PREMIS metadata about media objects.
- A JavaScript web application, written in React[56], used for creating and accessing the PREMIS data stored in the Ethereum smart contracts.

A working prototype of Provenator, as well as its source code, is available via the source code repository GitHub.[1]

The Working Prototype

The working prototype of Provenator exists on the network of the InterPlanetary File System (IPFS). IPFS is a peer-to-peer, content-addressed file system that forms the final component of our application's architecture; by publishing there, it means that the application is wholly distributed because, as discussed above, its underlying database, the blockchain, is also distributed. Furthermore, IPFS deploys cryptographic tools to ensure the authenticity of resources stored on its network. Thus, it is a good match for our technology. Below is a brief description of IPFS.

---

1 The address of the GitHub repository is https://github.com/glowkeeper/Provenator.

The InterPlanetary File System

IPFS deploys a generalisation of a Merkle directed acyclic graph (DAG) to establish a decentralised network of trusted data. Applying cryptographic hashes to a graph was Ralph Merkel's solution for transferring reliable information over an untrusted network[57]. The idea was profound; many systems that rely on trust employ Merkle DAGs - IPFS and Bitcoin[58] are just two examples among many. The fundamental principle behind a Merkle DAG is that if you have the hash of the root node, and the hash came from a trusted source, then, as long as the hashes match that of the root, you can trust all leaf nodes[42]. IPFS deploys a Merkle DAG to represent links between objects, which are cryptographic hashes of target blocks on the filesystem[59], a concept it has borrowed from the version control system Git[60]. Figure 10 shows the representation of an image on IPFS. Hence, any file stored under IPFS is guaranteed to be unique. Moreover, as long as the file forms a Merkle DAG of objects, it can be trusted, too. Furthermore, because new objects hash differently, objects on IPFS are, essentially, immutable[59].

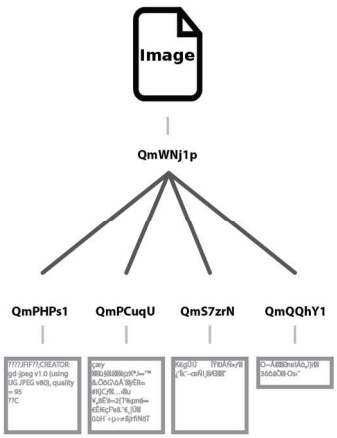


Figure 10. A Hash Tree[61]

Nodes on the IPFS network, which connect to one another to transfer and store objects, can be considered as trusted sources since they use public-key cryptography to establish their identity; they do so by using a cryptographic hash of the public half of their public and private key pair. When two nodes connect, they do so by exchanging those public keys, which are then used to encrypt subsequent communication. IPFS nodes generate their key pairs using the asymmetric cryptographic algorithm RSA[62], which uses random numbers via entropy sources of the IPFS nodes themselves. RSA's security relies on the properties of the integer factorisation problem (IFP):

Given $n = pq$, find p and q, where p and q are primes.

IFP looks deceptively simple. However, provided that p and q are sufficiently large, solving it is, actually, computationally infeasible[39].

Not So Smart Contracts

At the time of writing, the working prototype of Provenator uses the Ethereum Testnet, Ropsten[63]. However, we hope to produce a viable production release, so it may be that, by the time of publication, the application is running on the Ethereum blockchain itself. If that is the case, then Ethereum transactions that update the blockchain cost Ether (the unit of currency on Ethereum), so there will be a fee for storing metadata about digital resources.

Appendix G of the Ethereum yellow paper details some reasonably complex calculations for determining the fee schedule of Ethereum transactions[64]. However, the essence of those fees is less code leads to less cost. Furthermore, retrieving

information from the blockchain is free. That leads to some important design decisions when building a distributed application (dApp); not least is that the JavaScript web application, which serves as the user interface, should do much of the heavy lifting and the smart contracts should only set and get, rendering them not so smart, after all. An example will serve to illustrate - when adding a media resource to Provenator, the user must also input the agent, or content creator, who owns that resource. A reasonable application design would be to send that agent information to the smart contracts and have them check whether the agent already exists in the database. However, that check, if it leads to a blockchain update, could be prohibitively expensive. A less costly design is to have the smart contracts expose a simple accessor method for retrieving agent data from an index of agents - an operation that can be carried out for free. That way, the web application can use the accessor method to perform the same check for nothing and only pay for agent data to be stored on the blockchain if the agent does not already exist.

Use of Provenator

Consider the situation we described in the introduction to this paper, whereby the supporter of the then-Republican candidate for the U.S. Presidency published a photograph of a man behind some ballot boxes as an accompaniment to a claim that the Democrats were rigging votes. Figure 11 below shows a screenshot from of the Christian Times website making that claim.

Figure 11. A Snapshot of the Christian Times Website, Where it was Claimed the Clinton's Were Rigging Votes. Picture Courtesy of The New York Times[3]

The exchangeable image file format (Exif), is a standard for specifying information about image files[65], including data such as descriptions and copyright information. Unfortunately, such data is easily changed[66]. Presumably, the editor of the Christian Times did just that, and therefore, the New York Times had to go to great lengths to prove out of context use of the image. Now imagine that Alice was the photographer who took that photograph and that she used Provenator to record data about the

picture on the blockchain. Under that circumstance, proving that the Christian Times had used Alice's picture falsely would be a simple matter of using Provenator. Thus, the New York Times could have saved itself much bother.

Next, we discuss the schema Alice uses to register herself, using Provenator, as the creator of that photograph.

Provenator's PREMIS Metadata

Figure 12 below shows Alice using Provenator's PREMIS data model[50] to create information about her photo, which she stores on the blockchain. She records a cryptographic hash of her picture, along with associated metadata (such as a description of the image), as a PREMIS object. She also records the date the photo was taken, as a PREMIS event. The PREMIS agent describes Alice herself. The PREMIS rights detail the image's license.

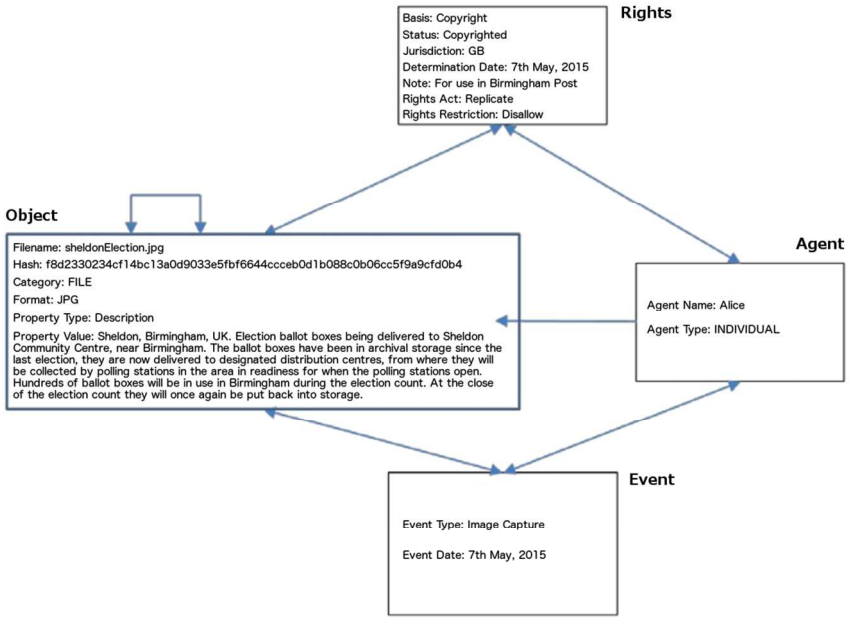


Figure 12. The PREMIS 3.0 data model[50] Applied to Alice's Picture of the Sheldon Election Ballot Boxes

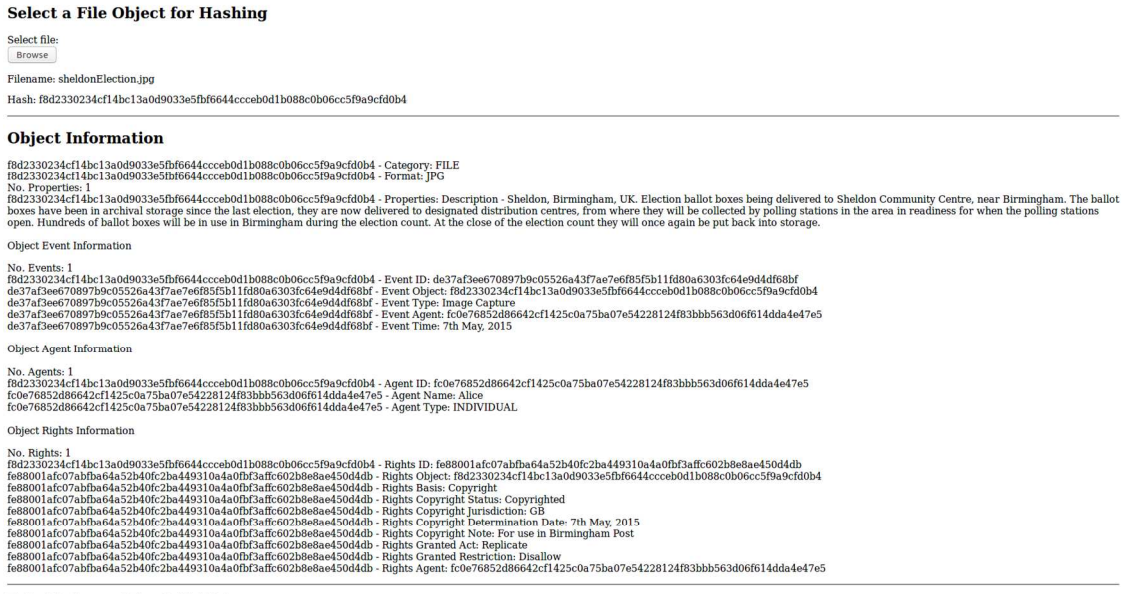
The implementation of the metadata, which we show above, describes a single object - Alice's picture of the ballot boxes used in the Sheldon election. That object has a single agent - Alice herself. It has a single event - the date when the picture was taken, and a single right - the Birmingham Post's copyright. However, the implementation of the PREMIS metadata used by Provenator is more complex. It describes a PREMIS object that can have many properties, as well as many agents, events and rights (for example, the licensing rights may be different in the UK to those in the U.S.). Similarly, although an event may only belong to a single agent, an agent may record multiple events, own many objects and deploy many different rights. Finally, specific rights belong to a single object and a single agent.

MetaMask

MetaMask[67] is a tool able to run an Ethereum dApp in a browser. When using Provenator, Alice can use MetaMask to sign the transactions she creates for storing the PREMIS metadata about her picture on the blockchain. By doing so, anyone accessing that data is confident that it was Alice herself who recorded the information.

Viewing The PREMIS Data

Now Alice has recorded information about her photograph, Bob, her eEditor, can use the image Alice sends to generate a cryptographic hash and retrieve information about that hash from the blockchain. Figure 13 shows a screenshot of Provenator, after Bob has recovered data about the picture Alice sent to him.



Select a File Object for Hashing

Select file:
Browse

Filename: sheldonElection.jpg

Hash: f8d2330234cf14bc13a0d9033e5fbf6644ccceb0d1b088c0b06cc5f9a9cfd0b4

Object Information

f8d2330234cf14bc13a0d9033e5fbf6644ccceb0d1b088c0b06cc5f9a9cfd0b4 - Category: FILE
f8d2330234cf14bc13a0d9033e5fbf6644ccceb0d1b088c0b06cc5f9a9cfd0b4 - Format: JPG
No. Properties: 1
f8d2330234cf14bc13a0d9033e5fbf6644ccceb0d1b088c0b06cc5f9a9cfd0b4 - Properties: Description - Sheldon, Birmingham, UK. Election ballot boxes being delivered to Sheldon Community Centre, near Birmingham. The ballot boxes have been in archival storage since the last election, they are now delivered to designated distribution centres, from where they will be collected by polling stations in the area in readiness for when the polling stations open. Hundreds of ballot boxes will be in use in Birmingham during the election count. At the close of the election count they will once again be put back into storage.

Object Event Information

No. Events: 1
f8d2330234cf14bc13a0d9033e5fbf6644ccceb0d1b088c0b06cc5f9a9cfd0b4 - Event ID: de37af3ee670897b9c05526a43f7ae7e6f85f5b11fd80a6303fc64e9d4df68bf
de37af3ee670897b9c05526a43f7ae7e6f85f5b11fd80a6303fc64e9d4df68bf - Event Object: f8d2330234cf14bc13a0d9033e5fbf6644ccceb0d1b088c0b06cc5f9a9cfd0b4
de37af3ee670897b9c05526a43f7ae7e6f85f5b11fd80a6303fc64e9d4df68bf - Event Type: Image Capture
de37af3ee670897b9c05526a43f7ae7e6f85f5b11fd80a6303fc64e9d4df68bf - Event Agent: fc0e76852d86642cf1425c0a75ba07e54228124f83bbb563d06f614dda4e47e5
de37af3ee670897b9c05526a43f7ae7e6f85f5b11fd80a6303fc64e9d4df68bf - Event Time: 7th May, 2015

Object Agent Information

No. Agents: 1
f8d2330234cf14bc13a0d9033e5fbf6644ccceb0d1b088c0b06cc5f9a9cfd0b4 - Agent ID: fc0e76852d86642cf1425c0a75ba07e54228124f83bbb563d06f614dda4e47e5
fc0e76852d86642cf1425c0a75ba07e54228124f83bbb563d06f614dda4e47e5 - Agent Name: Alice
fc0e76852d86642cf1425c0a75ba07e54228124f83bbb563d06f614dda4e47e5 - Agent Type: INDIVIDUAL

Object Rights Information

No. Rights: 1
f8d2330234cf14bc13a0d9033e5fbf6644ccceb0d1b088c0b06cc5f9a9cfd0b4 - Rights ID: fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db
fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db - Rights Object: f8d2330234cf14bc13a0d9033e5fbf6644ccceb0d1b088c0b06cc5f9a9cfd0b4
fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db - Rights Basis: Copyright
fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db - Rights Copyright Status: Copyrighted
fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db - Rights Copyright Jurisdiction: GB
fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db - Rights Copyright Determination Date: 7th May, 2015
fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db - Rights Copyright Note: For use in Birmingham Post
fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db - Rights Granted Act: Replicate
fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db - Rights Granted Restriction: Disallow
fe88001afc07abfba64a52b40fc2ba449310a4a0fbf3affc602b8e8ae450d4db - Rights Agent: fc0e76852d86642cf1425c0a75ba07e54228124f83bbb563d06f614dda4e47e5

Finished fetching records from the blockchain.

Figure 13. Screenshot of Bob Using Provenator to Retrieve Information About Alice's Picture. Source: Authors' own work, whereby the scenario depicted in this paper has been recreated.

Due to the deterministic and collision resistance properties of cryptographic hashes, by retrieving the data above, Bob is confident as to the authenticity of the image Alice sent. He can also apply edits and record information about those changes, thus creating a provenance chain for the picture. Hence, rather than going to great investigative lengths to prove out of context use of Alice's image, the New York Times would have been able to check the validity of the picture simply by uploading the Christian Times' copy to Provenator. Then they would have retrieved the same metadata as Bob, which would have shown the picture to be fake.

However, although that would have shown the image itself was fake, it would not have proved that the article as a whole was fiction. Proving that might take a little more than technology. We consider that issue, next.

Validating News

The BBC has had many difficulties in providing accurate news stories from behind the frontlines of the Syrian conflict[68]. Indeed, journalists have lost their lives there, so it has become common practice to source stories from ordinary Syrian citizens. However, ensuring the validity of such 'user-generated content' (UGC) has been "a skill journalists have had to learn"[68]. To that end, the BBC has become proficient at developing new practices that ensure the validity of UGC content. Apparently, such methods involve technology, but also common sense and fostering healthy relationships with reliable Syrians[68]. Augmenting big data news stream technology with a 'human touch' to verify items is a common theme[69]. For example, one project argues for the formation of a fake news corpus to aid deception detection, and to that end, when collecting the data, qualified participants will be required to spot the fakes[33]. In fact, all of the big data technologies we mentioned above require some form of human action - either through visualising graphs or acting upon some visual data. Therein lies the crucial point; when the BBC check the validity of stories given by users behind the Syrian front lines, technology can only go so far. A good deal of human skill is required, too. Moreover, while technology, such as Provenator, will make it possible to prove the validity of media resources used within news, proving the authenticity of fake news stories as a whole often takes good journalistic practices. Another good example is the experience of Facebook; while countering propaganda in the run-up to the 2016 U.S. Election, the company found that their algorithms were not always up to the job of spotting fake stories. Instead, to curate the news items appearing on their site, they had to fall back on human editors[70].

Current Limitations of Provenator and Future Work

A strength of Provenator is also a weakness. The strength is that the same digital media resource will always generate the same cryptographic hash. Thus, if two hashes match, it is certain that it is the same object. Therefore, we can retrieve provenance data and trust that it accurately reflects the object's origins. To put that another way, changing a single pixel in a digital resource will generate an entirely different cryptographic hash. Therein lies the weakness - it would not have been difficult for the Christian Times to alter the image of the Sheldon Election ballot boxes, thus, as it stands, defeating our tool.

However, that weakness in our early prototype of Provenator is not insurmountable. For example, it may be possible to use some form of mathematical filter to remove or reduce the 'noise' of an object, thus rendering two seemingly disparate resources, identical[71]. There may be better approaches than filtering, however. Narwal et al. describe how they classify similar images using fisher vectors and k-means clustering[36]. Indeed, object classification via fisher vectors appears to be an active area of computer vision research[72]. Hence, if Provenator used such techniques, users may be able to classify images, discover similarities and find fakes that way. Furthermore, fisher vectors are used for classifying videos, too[73], so Provenator's scope could broaden beyond images. That could be true for another technique, too - perceptual hashes[74], which establish object matches based on perceived content[75]. Whereas any change in two multimedia resources will generate vastly different cryptographic hashes, perceptual hashes produce comparable results if the resources are similar. Hence, if future versions of Provenator extend its

resource metadata to include a perceptual hash, that single pixel change above would render a complimentary perceptual hash that can be matched against the original by calculating their hamming distance[76]. Indeed, perceptual hashing is already used by organisations such as Shazam, Google and also by Youtube to detect copyright infringement across a broad range of digital objects, such as audio, video and images[75]. Indeed, although this paper uses the example of a picture to help explain the application's functionality, Provenator can be used to prove the provenance of any media objects, even the news stories themselves. In fact, improvements in future versions, using methods such as fisher vectors and or perceptual hashes, would make it even more suitable as a tool for helping to prove the origins of different media resources.

Conclusion

Fake news has hit the headlines recently. Indeed, Donald Trump has continued to accuse various media outlets of distributing falsehoods that undermine him[77]. We have not examined the reasons for his doing so; such an examination would be interesting, but it is not the focus of this paper. Moreover, although we have given some background history on the issue of fake news, it is beyond the scope of this article to discuss propaganda itself. Additionally, although we discuss the issue of social media platforms and fake news, we do not examine the methods and processes for distributing fake news items on such platforms or the efficacy of the measures taken by those platforms to counter the problem. Instead, the purpose of this paper has been to propose a technological solution to the problem of proving the validity of media resources used in fake news. Various research groups are

investigating technologies capable of overcoming the problem of verifying big data news streams. However, the application we have developed, Provenator, is uniquely capable of recording metadata about digital media on blockchain technology so that it becomes trivial to prove their authenticity in a manner that can be trusted. The ultimate aim of our tool is to make content creators accountable for the resources they create.

Unfortunately, as it stands, although Provenator works well for recording the origins of a media resource, it is easy to defeat the 'find fake' capabilities of this early prototype, simply by changing a single pixel of a misappropriated image. That may be addressed in future version, since there are techniques available, such as fisher vectors and perceptual hashes, which can improve future versions of the application and make it much more capable.

However, while Provenator may become more proficient at verifying the authenticity of media resources used within a story, the application will only ever be capable of providing a partial solution to the problem of fake news. Unfortunately, we do not think technology will ever be wholly capable of proving the truth of the story as a whole. We believe, currently, that takes human skills. Certainly, while it might take some sophisticated mathematics to determine the similarity between two media resources that only differ by a single pixel, the same complexity does not apply to the human eye, which would quickly decide that those resources are the same.

Although we have reservations about the possible limitations of technology in combating fake news, we believe the trust mechanisms of blockchains make them better positioned than other technologies for proving the authenticity of media resources. Indeed, organisations are investigating using blockchains for purposes such as transparency and publicly auditable content ranking[78]. Moreover, our application is an example of a tool that can help fight 'fakeness'. Indeed, in our supposed scenario, where Alice was the photographer who took the image used by the Christian Times, The New York Times would have had a much easier job of proving falsehood.

Acknowledgements

The idea for this paper came after a discussion over tea with colleagues at the University of Sussex; namely, Phil Watten and Patrick Holroyd. Thank you also to Ian Wakeman, Head of Informatics at the University of Sussex, who provided feedback on the first draft of the paper and, in particular, provided useful references on image capture. Also thank you to Konstantin Blyuss, reader in Mathematics at the University of Sussex, who provided insight about cryptography. Finally, we're grateful to the anonymous reviewers, as well as the editors, who gave suggestions that improved the paper immeasurably.

References

1. Watts AW. How Russia Dominates Your Twitter Feed to Promote Lies (And, Trump, Too) [Internet]. The Daily Beast. 2016–2016-08-06T04:03:00.000Z [cited 2017 Feb 5]. Available from: http://www.thedailybeast.com/articles/2016/08/06/how-russia-dominates-your-twitter-feed-to-promote-lies-and-trump-too.html

2. Morin R. Trump: New York Times is 'fake news' [Internet]. POLITICO. 17AD [cited 2017 Feb 5]. Available from: http://politi.co/2jAdgwn

3. Shane S. From Headline to Photograph, a Fake News Masterpiece. The New York Times [Internet]. 2017 Jan 18 [cited 2017 Feb 5]; Available from: https://www.nytimes.com/2017/01/18/us/fake-news-hillary-clinton-cameron-harris.html

4. Walker J. Birmingham Mail photo used in a 'fake news' Trump story shared with 6 million [Internet]. birminghammail. 2017 [cited 2017 Sep 27]. Available from: http://www.birminghammail.co.uk/news/midlands-news/birmingham-mail-photo-used-fake-12476900

5. Hunt E. What is fake news? How to spot it and what you can do to stop it. The Guardian: Media [Internet]. 2016 Dec 17 [cited 2017 Feb 27]; Available from: https://www.theguardian.com/media/2016/dec/18/what-is-fake-news-pizzagate

6. Jessica Goodfellow. Only 4% of people can distinguish fake news from truth, Channel 4 study finds [Internet]. The Drum. 2017 [cited 2017 Mar 23]. Available from: http://www.thedrum.com/news/2017/02/06/only-4-people-can-distinguish-fake-news-truth-channel-4-study-finds

7. Foo Yun Chee. NATO says it's seen a sharp rise in Russian fake news since the Kremlin seized Crimea [Internet]. Business Insider. 2017 [cited 2017 Apr 20]. Available from: http://uk.businessinsider.com/r-nato-says-it-sees-sharp-rise-in-russian-disinformation-since-crimea-seizure-2017-2

8. Fake news series part two [Internet]. Channel 4 News. 19:00 00:41:21-00:55:54: Channel 4; 2017. Available from: https://learningonscreen.ac.uk/ondemand/index.php/clip/90422

9. MacIntyre D. Facebook - the secret election weapon. BBC News: UK [Internet]. 20172017-05-08T02:52:38+01:00 [cited 2017 May 8]; Available from: http://www.bbc.co.uk/news/uk-39830727

10. Silverman C. This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook [Internet]. BuzzFeed. 2016 [cited 2017 May 9]. Available from: https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook

11. Jen Weedon, William Nuland, Alex Stamos. Facebook and Information Operations [Internet]. Facebook; 2017 [cited 2017 May 8]. Available from: https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf

12. Cellan-Jones R. Facebook publishes fake news ads in UK papers. BBC News: Technology [Internet]. 20172017-05-08T05:00:25+01:00 [cited 2017 May 8]; Available from: http://www.bbc.co.uk/news/technology-39840803

13. Mark Zuckerberg. What we're doing about misinformation [Internet]. 2016 [cited 2017 May 9]. Available from: https://www.facebook.com/zuck/posts/10103269806149061?pnref=story

14. reporter AHT. Wikipedia founder to fight fake news with new Wikitribune site. The Guardian: Technology [Internet]. 2017 Apr 25 [cited 2017 May 8]; Available from: https://www.theguardian.com/technology/2017/apr/25/wikipedia-founder-jimmy-wales-to-fight-fake-news-with-new-wikitribune-site

15. Nationalism vs. globalism: The new political divide [Internet]. 2017 [cited 2017 Mar 3]. Available from: http://www.ted.com/talks/yuval_noah_harari_nationalism_vs_globalism_the_new_political_divide

16. Nagle DB, Burstein SM, editors. The ancient world: Readings in social and cultural history. 4th ed. New York: Prentice Hall; 2010. 280 pp.

17. Online Etymology Dictionary. Propaganda [Internet]. 2017 [cited 2017 Mar 27]. Available from: http://www.etymonline.com/index.php?term=propaganda

18. Dr David Clarke. The corpse factory and the birth of fake news. BBC News: Entertainment & Arts [Internet]. 20172017-02-17T08:29:53+00:00 [cited 2017 Feb 25]; Available from: http://www.bbc.co.uk/news/entertainment-arts-38995205

19. A-Z Quotes. Joseph Goebbels Quote [Internet]. A-Z Quotes. 2017 [cited 2017 Mar 4]. Available from: http://www.azquotes.com/quote/1419276

20. Davies S. Popular opinion in Stalin's Russia: Terror, propaganda, and dissent, 1934-1941. Cambridge ; New York: Cambridge University Press; 1997. 236 pp.

21. Zasurskiĭ I. Media and power in post-Soviet Russia. Armonk, N.Y: M.E. Sharpe; 2004. 269 pp.

22. Jane's 360. Acknowledgement of Russia's information warfare capability indicates its strategic importance and impracticability of maintaining plausible [Internet]. 2017 [cited 2017 May 4]. Available from: http://www.janes.com/article/68267/acknowledgement-of-russia-s-information-warfare-capability-indicates-its-strategic-importance-and-impracticability-of-maintaining-plausible-deniability-policy

23. Khaldarova I, Pantti M. Fake News: The narrative battle over the Ukrainian conflict. Journalism Practice [Internet]. 2016 Oct 2 [cited 2017 Mar 2];10(7):891–901. Available from: https://www.tandfonline.com/doi/full/10.1080/17512786.2016.1163237 (DOI: 10.1080/17512786.2016.1163237)

24. Bernays EL, Miller MC. Propaganda. Brooklyn, N.Y: Ig Publishing; 2005. 168 pp.

25. McChesney RW, Wood EM, Foster JB, editors. Capitalism and the information age: The political economy of the global communication revolution. New York, NY: Monthly Review Press; 1998. 254 pp.

26. Office of the Historian. Foreign Relations of the United States, 1945–1950, Emergence of the Intelligence Establishment [Internet]. 1948 [cited 2017 May 4]. Available from: https://history.state.gov/historicaldocuments/frus1945-50Intel/d292

27. Robert Love. Before Jon Stewart [Internet]. Columbia Journalism Review. 2007 [cited 2017 Mar 1]. Available from: http://www.cjr.org/feature/before_jon_stewart.php

28. Orwell G. 1984: A novel; revised and updated bibliography. New York [u.a.: New American Library; 1985.

29. Staff LII. First Amendment [Internet]. LII / Legal Information Institute. 2010 [cited 2017 Mar 1]. Available from: https://www.law.cornell.edu/constitution/first_amendment

30. Fixing the News [Internet]. 2015 [cited 2017 May 4]. (TEDxVancouver). Available from: https://www.youtube.com/watch?v=NwmGTM5Py8Y

31. boyd danah, Crawford K. Six Provocations for Big Data. SSRN Electronic Journal [Internet]. 2011 [cited 2017 Sep 20]; Available from: http://www.ssrn.com/abstract=1926431 (DOI: 10.2139/ssrn.1926431)

32. Labrinidis A, Jagadish HV. Challenges and opportunities with big data. Proceedings of the VLDB Endowment [Internet]. 2012 Aug 1 [cited 2017 Sep 20];5(12):2032–3. Available from: http://dl.acm.org/citation.cfm?doid=2367502.2367572 (DOI: 10.14778/2367502.2367572)

33. Rubin VL, Chen Y, Conroy NJ. Deception detection for news: Three types of fakes: Deception Detection for News: Three Types of Fakes. Proceedings of the Association for Information Science and Technology [Internet]. 2015 [cited 2017 Sep 21];52(1):1–4. Available from: http://doi.wiley.com/10.1002/pra2.2015.145052010083 (DOI: 10.1002/pra2.2015.145052010083)

34. QUENTIN VIEREGGE. Journalism: Gathering Information and Writing Your Story [Internet]. 2017 [cited 2017 Apr 12]. Available from: https://writingcommons.org/open-text/research-methods-methodologies/empirical-research/interviews/journalism-gathering-information-and-writing-your-story

35. Ed Grover. City journalism academics to lead European big data and fake news project [Internet]. City, University of London. 7th July 2017 [cited 2017 Sep 21].

Available from: https://www.city.ac.uk/news/2017/june/google-digital-news-initiative-dminr

36. Narwal V, Salih MH, Lopez JA, Ortega A, O'Donovan J, Höllerer T, et al. Automated Assistants to Identify and Prompt Action on Visual News Bias. In ACM Press; 2017 [cited 2017 Sep 22]. pp. 2796–801. Available from: http://dl.acm.org/citation.cfm?doid=3027063.3053227 (DOI: 10.1145/3027063.3053227)

37. Jin Z, Cao J, Jiang Y-G, Zhang Y. News Credibility Evaluation on Microblog with a Hierarchical Propagation Model. In IEEE; 2014 [cited 2017 Sep 22]. pp. 230–9. Available from: http://ieeexplore.ieee.org/document/7023340/ (DOI: 10.1109/ICDM.2014.91)

38. Menezes AJ, Van Oorschot PC, Vanstone SA. Handbook of applied cryptography. Boca Raton: CRC Press; 1997. 780 pp. (CRC press series on discrete mathematics and its applications).

39. Dr Konstantin Blyuss. Cryptography - Lecture Notes. 2016.

40. Ethereum. Ethereum Glossary [Internet]. GitHub. 2016 [cited 2017 Mar 22]. Available from: https://github.com/ethereum/wiki

41. KohanX. Public Key Cryptography [Internet]. 2010. Available from: https://commons.wikimedia.org/wiki/File:Public-key-crypto-1.svg

42. Tyler Cipriani. Visualizing Git's Merkle DAG with D3.Js - Tyler Cipriani [Internet]. 2016 [cited 2017 Mar 13]. Available from: https://tylercipriani.com/blog/2016/03/21/Visualizing-Git-Merkle-DAG-with-D3.js/

43. Bitcoin Wiki. Elliptic Curve Digital Signature Algorithm [Internet]. 2015 [cited 2017 Mar 27]. Available from: https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm

44. Swan M. Blockchain: Blueprint for a New Economy. "O'Reilly Media, Inc." 2015. 149 pp.

45. Umeh J. Blockchain Double Bubble or Double Trouble? ITNOW [Internet]. 2016 Mar [cited 2017 Feb 5];58(1):58–61. Available from: https://academic.oup.com/itnow/article-lookup/doi/10.1093/itnow/bww026 (DOI: 10.1093/itnow/bww026)

46. Huckle S, White M. Socialism and the Blockchain. Future Internet [Internet]. 2016 Oct 18 [cited 2016 Nov 7];8(4):49. Available from: http://www.mdpi.com/1999-5903/8/4/49 (DOI: 10.3390/fi8040049)

47. Eris Industries. Explainer | Smart Contracts [Internet]. Eris Industries Documentation. 2016 [cited 2016 Mar 19]. Available from: https://docs.erisindustries.com/explainers/smart_contracts/

48. The Economist. The trust machine. The Economist [Internet]. 2015 Oct 31 [cited 2016 Feb 17]; Available from: http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

49. Priscilla Caplan. Understanding PREMIS [Internet]. The Library of Congress; 2009 [cited 2017 Sep 23]. Available from: https://www.loc.gov/standards/premis/understanding-premis.pdf

50. PREMIS Editorial Committee. The PREMIS Data Dictionary Version 3.0 [Internet]. 2015 [cited 2017 Jun 29]. Available from: https://www.loc.gov/standards/premis/v3/premis-3-0-final.pdf

51. W3C. Data on the Web - Best Practices [Internet]. 2015 [cited 2017 May 11]. Available from: https://www.w3.org/TR/2015/WD-dwbp-20150224/

52. Mannens E, Coppens S, Verborgh R, Hauttekeete L, Van Deursen D, Van de Walle R. Automated Trust Estimation in Developing Open News Stories: Combining Memento and Provenance. In IEEE; 2012 [cited 2017 Sep 22]. pp. 122–7. Available from: http://ieeexplore.ieee.org/document/6341562/ (DOI: 10.1109/COMPSACW.2012.32)

53. Ubuntu. VerifyIsoHowto - Community Help Wiki [Internet]. 2016 [cited 2017 Mar 11]. Available from: https://help.ubuntu.com/community/VerifyIsoHowto

54. Ethereum. Ethereum Project [Internet]. 2017 [cited 2017 Jan 10]. Available from: https://www.ethereum.org/

55. Solidity. Solidity — Solidity 0.4.8-develop documentation [Internet]. 2016 [cited 2017 Jan 13]. Available from: https://solidity.readthedocs.io/en/develop/

56. React. React - A JavaScript library for building user interfaces [Internet]. 2017 [cited 2017 Jun 29]. Available from: https://facebook.github.io/react/

57. Merkle RC. A Digital Signature Based on a Conventional Encryption Function. In: Pomerance C, editor. Advances in Cryptology — CRYPTO '87 [Internet]. Berlin, Heidelberg: Springer Berlin Heidelberg; 1988 [cited 2017 Mar 13]. pp. 369–78. Available from: http://link.springer.com/10.1007/3-540-48184-2_32 (DOI: 10.1007/3-540-48184-2_32)

58. Bitcoin. Bitcoin - Open source P2P money [Internet]. 2015 [cited 2015 Nov 27]. Available from: https://bitcoin.org/en/

59. Juan Benet. IPFS - Content Addressed, Versioned, P2P File System (DRAFT 3) [Internet]. 2017 [cited 2017 Mar 13]. Available from:

https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf

60. Git. Git [Internet]. 2017 [cited 2017 Mar 13]. Available from: https://git-scm.com/

61. flyingzumwalt. The Decentralized Web Primer - Lesson: Turn a File into a Merkle Tree [Internet]. 2016 [cited 2017 Mar 13]. Available from: https://flyingzumwalt.gitbooks.io/decentralized-web-primer/content/ipfs-dag/lessons/files-as-dags.html

62. Dell EMC. RSA Laboratories - PKCS #1: RSA Cryptography Standard [Internet]. 2017 [cited 2017 May 23]. Available from: https://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs-rsa-cryptography-standard.htm

63. Ethereum. Ropsten: Ropsten public testnet PoW chain [Internet]. ethereum; 2017 [cited 2017 Jul 16]. Available from: https://github.com/ethereum/ropsten

64. Gavin Wood. ETHEREUM - A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. EIP-150 REVISION [Internet]. 2013 [cited 2017 Jan 16]. Available from: http://gavwood.com/paper.pdf

65. EXIF.org. EXIF and related resources [Internet]. 2017 [cited 2017 Sep 26]. Available from: http://www.exif.org/

66. Mauro Huculak. How to edit image metadata on Windows 10 [Internet]. Windows Central. 2017 [cited 2017 Sep 26]. Available from: https://www.windowscentral.com/how-edit-picture-metadata-windows-10

67. MetaMask. MetaMask [Internet]. 2017 [cited 2017 Mar 28]. Available from: https://metamask.io/

68. Lisette Johnston. How is citizen journalism transforming the BBC's Newsroom practices? [Internet]. 2017. Available from: https://www.academia.edu/20427847/How_is_citizen_journalism_transforming_the_BBC_s_Newsroom_practices

69. Sethi RJ. Crowdsourcing the Verification of Fake News and Alternative Facts. In ACM Press; 2017 [cited 2017 Sep 21]. pp. 315–6. Available from: http://dl.acm.org/citation.cfm?doid=3078714.3078746 (DOI: 10.1145/3078714.3078746)

70. McHugh M. Facebook Can Try to Fix Fake News, but It Can Never Be an Arbiter of Truth [Internet]. The Ringer. 2016 [cited 2017 May 9]. Available from: https://theringer.com/facebook-can-try-to-fix-fake-news-but-it-can-never-be-an-arbiter-of-truth-75d4d0ca0176#.9pdaniqlk

71. Datta R, Joshi D, Li J, Wang JZ. Image retrieval: Ideas, influences, and trends of the new age. ACM Computing Surveys [Internet]. 2008 Apr 1 [cited 2017 Jul

24];40(2):1–60. Available from: http://portal.acm.org/citation.cfm?doid=1348246.1348248 (DOI: 10.1145/1348246.1348248)

72. Liu L, Wang P, Shen C, Wang L, van den Hengel A, Wang C, et al. Compositional Model Based Fisher Vector Coding for Image Classification. IEEE Transactions on Pattern Analysis and Machine Intelligence [Internet]. 2017 [cited 2017 Sep 24];1–1. Available from: http://ieeexplore.ieee.org/document/7812753/ (DOI: 10.1109/TPAMI.2017.2651061)

73. Sun C, Nevatia R. Large-scale web video event classification by use of Fisher Vectors. In IEEE; 2013 [cited 2017 Sep 24]. pp. 15–22. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6474994 (DOI: 10.1109/WACV.2013.6474994)

74. Joe Bertolami. Perceptual Hashing [Internet]. Wednesday, May 28th, 2014 [cited 2017 Sep 24]. Available from: http://bertolami.com/index.php?engine=blog&content=posts&detail=perceptual-hashing

75. rfraimow. Adventures in Perceptual Hashing [Internet]. AAPB National Digital Stewardship Residency. 2017–2017-04-20T14:27:45+00:00 [cited 2017 Sep 24]. Available from: https://ndsr.americanarchive.org/2017/04/20/adventures-in-perceptual-hashing/

76. Hamming RW. Error Detecting and Error Correcting Codes. Bell System Technical Journal [Internet]. 1950 Apr [cited 2017 Sep 27];29(2):147–60. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6772729 (DOI: 10.1002/j.1538-7305.1950.tb00463.x)

77. Nikki Schwab. Trump calls NBC and ABC 'totally biased and fake news' AGAIN [Internet]. Mail Online. 2017 [cited 2017 Mar 28]. Available from: http://www.dailymail.co.uk/~/article-4342518/index.html

78. Jill Richmond. Using Blockchain Technology to Fight Fake News [Internet]. Distributed. 2017 [cited 2017 Jul 16]. Available from: /news/how-blockchain-can-fight-fake-news/